



GISRA and GPEA Overview

February 12, 2002



GISRA Overview

- Risk Assessment
 - Independent review and test of security controls.
- Security Plan
 - Describes system's security procedures and controls.
 - Includes: Continuity of Operations Plan (COOP), Disaster Recovery Plan (DRP), Configuration Management plan, and Rules of Behavior (RoB).
- Certification and Accreditation (C&A)
 - Validation testing of system's security procedures and controls.
 - Includes: Risk Assessment results, Configuration Management plan, COOP/DRP, Security Testing & Evaluation (ST&E) plan and results, and System Security Authorization Agreement (SSAA).



Primary GISRA Milestones

Risk Assessment	Security Plan	C&A
<p>Due Date: 4/15/02</p> <p>Funding: \$25K-125K/system</p> <ul style="list-style-type: none">• 18 systems on FSA inventory• 5 systems under compliance review• Several to be retired within the next year <p>Total estimated cost (excluding 5 completed): \$850K</p> <p>Staff: FSA oversight and staff plus 2-5 independent contractor employees</p>	<p>Due Date: 6/15/02</p> <p>Funding: \$10K-60K/system</p> <p>Total estimated cost: \$540K</p> <p>Staff: FSA oversight and staff plus 1-3 contractor employees</p>	<p>Due Date: 12/15/02 (assumed)</p> <p>Funding: Indeterminable</p> <p>Staff: Indeterminable</p> <p>Funding and staff requirements will be able to be determined after receiving Ed guidance (mid-March, 2002)</p>



GISRA Concerns and Resolution Recommendations

- ED compliance dates set well after FY02 budget determined.
 - Push back C&A completion to allow use of FY03 budget and time?
- Departmental task completion criteria changing “on-the-fly.”
 - Clarification regarding use of independent RA received 2/5/02; only two months reaction time to hire contractors, complete RA.
- No ED guidance yet for C&A requirements, format, etc.
 - Unknown testing requirements, format, necessary documentation, etc. precludes budgeting and planning process.
- Scope and interrelationship of FSA systems necessitate more time and funding to complete tasks than for other agencies’ systems.



GPEA

- FSA is already dedicated to “moving from paper to electrons.”
- We need to ensure we comply with GPEA reporting requirements.